1729

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,503	05/03/2001	Cheman Shaik		7862

7590 12/23/2004

Shaik Cheman
P.O. Box 56565
Riyadh,
SAUDI ARABIA

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/847,503	**Applicant(s)** SHAIK, CHEMAN	
	Examiner Jung W Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 May 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-15 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: on page 10, line 23, the word "do" is misspelled. Appropriate correction is required.

Claim Objections

3. Claims 2, 3, 10 and 15 are objected to because of the following informalities: claims 2 and 3 refer to the methods of claim 1; however only one method is defined in claim 1; in claim 10, the word "least" is misspelled; claim 15 defines the limitation "t is a random number generated on encrypting machine and discarded after encryption is complete" (page 30, last line); however, "t" is not utilized by the invention define within the scope of claim 15. Appropriate correction is required.

4. Claims 2-9 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claims 2-9 reiterate method step(s) predefined in parent claim 1.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1, 10, 13 and 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim 1 recites the limitations "on encrypting unit" (limitation beginning with "t is a random number ..." and "the destination unit" (limitation beginning with "(b) delivering ..."). There is insufficient antecedent basis for these limitations in the claim.

8. Claim 10 recites the limitation "the main host". There is insufficient antecedent basis for this limitation in the claim.

9. Claim 13 recites the limitations "on encrypting machine" (limitation beginning with "t is a random number ..."), "the other key" and "the recipient", (limitation beginning with "(d.sub.1), (d.sub.2), ... "). There is insufficient antecedent basis for these limitations in the claim.

10. Claim 14 recites the limitations "the computer" (preamble) and "on encrypting machine" (limitation beginning with "t is a random number ..."). There is insufficient antecedent basis for these limitations in the claim.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-15 are rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. Claims 1-15 disclose a system for securely sending messages over a network between first and second computing units wherein r public (e.sub.1, e.sub.2, ... e.sub.r) and private (d.sub.1, d.sub.2, ... d.sub.r) key components (r > 1) are generated to encrypt a message M into r cipher versions using the RSA cipher steps of:

M.sub.1 = M.sup.(e.sub.1) mod n

M.sub.2 = M.sup.(e.sub.2) mod n

. . . . .

. . . . .

M.sub.r = M.sup.(e.sub.r) mod n, where

n = p*q, p and q are two prime numbers; the public key components are relatively prime and the modulus is the same for each cipher step; (claim 1, page 23, last line 14-page 24, line 2)

or

M.sub.1 = M.sub.(e.sub.1 + t) mod n

M.sub.2 = M.sup.(e.sub.2 + t) mod n

. . . . .

. . . . .

M.sub.r = M.sup.(e.sub.r + t) mod n, where n = p*q, p and q are two prime numbers; t is a random number and the modulus is the same for each cipher step; (claim 1, page 22, last line 10-page 23, line 6). Also, independent claims 13, 14 and 15 define equivalent cipher steps.

However, Moore teaches a common modulus protocol failure first identified by G. J. Simmons, wherein if a message is transmitted to two receivers having public keys that are relatively prime using RSA encryption where the encryption steps for the two cipher messages share a common modulus, then the message can be recovered without breaking the cryptosystem. See Moore, Judy H. "Protocol Failures in Cryptosystems"; section III, especially page 596, 1st paragraph. In the case of the cipher steps without the blinding factor of t, the public keys are relatively prime and hence, the message is trivially recoverable without the decryption key. In the case of the cipher steps implementing the blinding factor of t and any two values of e.sub.1 + t, e.sub.2 + t, ... e.sub.r + t are relatively prime, the message is trivially recoverable without the decryption key.

Allowable Subject Matter

12. The following is a statement of reasons for the indication of allowable subject matter: Prior art Moore teaches cryptosystems wherein a message is encrypted using RSA techniques into several ciphertext and each ciphertext is generated using a distinct encryption key but using a common modulus as the other ciphertext. However, Moore does not teach computing r components of encrypting key e.sub.1, e.sub.2, ..., e.sub.r

and r components of decrypting key d.sub.1, d.sub.2, ..., d.sub.r according to the following relations:

for blind-key:

a. (e.sub.1)(d.sub.1) + (e.sub.2)(d.sub.2) + ... + (e.sub.r)(d.sub.r) = (k.sub.1)(p-1)(q-1) + 1 and (d.sub.1) + ... + (d.sub.r) = (k.sub.2)(p-1)(q-1), where:

i. p and q are two prime numbers;

ii. k.sub.1 and k.sub.2 are suitable integers;

pg. 7, 3rd full paragraph-pg. 12.

for composite key:

b. (e.sub.1)(d.sub.1) + (e.sub.2)(d.sub.2) + ... + (e.sub.r)(d.sub.r) = (k.sub.1)(p-1)(q-1) + 1 and each of the values e.sub.1, e.sub.2, ..., e.sub.r has a common factor with (p-1)(q-1), but there is no common factor for all e.sub.1, e.sub.2, ..., e.sub.r where:

iii. p and q are two prime numbers;

iv. k.sub.1 is a suitable integer;

pg. 12, last paragraph-pg. 14.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shamir, Adi "RSA for Paranoids".

Miyazaki et al. U.S. Patent No. 6,810,122.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (571) 272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
December 16, 2004

Gilberto

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100